2021 ISCA Symposium on Security and Privacy in Speech Communication
10-12 November 2021, Online

Design Implications for Human-Machine Interactions from a Qualitative Pilot Study on Privacy

Anna Leschanowsky[1], *Birgit Brüggemeier*[2], *Nils Peters*[1]

[1]International Audio Laboratories Erlangen, University of Erlangen-Nuremberg, Germany
[2]Fraunhofer IIS, Erlangen, Germany

anna.leschanowsky@fau.de, birgit.brueggemeier@iis.fraunhofer.de,
nils.peters@audiolabs-erlangen.de

Abstract

There are only few qualitative studies investigating privacy in Human-Machine Interaction (HMI). We conducted an exploratory qualitative study with the aim to better understand factors that influence privacy in HMI and how they relate to privacy in Human-to-Human Interaction (HHI). From there, we derived recommendations that can help designers to promote informed decision making and improve data sharing processes. We discuss the main distinguishing factors that were found carrying out semi-structured interviews. First, HMI contexts miss flexibility and proper protection strategies such that users can not easily protect themselves similar to what they are used to in HHI. Second, users were able to easily evaluate benefits of sharing data while risks remained elusive and difficult to assess. Further research is needed to understand the impact of this imbalance on users' informed decision making.

Index Terms: privacy, qualitative research, human-machine interaction

1. Introduction

Currently, social science research on privacy in HMI reports mostly quantitative results [1, 2, 3]. While these studies show that individual and contextual factors influence perceptions and preferences linked to privacy, other factors might not have been measured and thus disregarded. A qualitative approach has the potential to give new insights and uncover disregarded patterns [4]. So far, only a few studies have been published using semi-structured interviewing for privacy research mostly focusing on voice assistants [5, 6, 7]. We aimed to better understand privacy in a broader context while keeping in mind that privacy itself is highly subjective and partly socially constructed [8]. We asked two research questions to better understand privacy in HMI and to derive design implications from those:

- How does privacy in HMI relate to human-to-human interaction (HHI)?
- Which factors influence peoples' evaluation of privacy and their decision making about disclosure in HMI?

2. Study Design

To tackle the research questions, we conducted semi-structured interviews, transcribed and coded them line-by-line [4]. We set up an interpretive design for our study, acknowledging that the coding process itself is generally subjective [4]. The coding was carried out by one researcher and the emerging categories were discussed in the group [4].

We based our first sample of interviewees on a mix of convenient and purposeful sampling [9]. Later in the process, we made use of theoretical sampling, a method of sampling based on theoretical grounds [4]. Thus, we first disregarded demographics in interviewee selection and later maximized some demographic differences to test for uniformities [4] (see Appendix 7.1). We stopped interviewing after nine interviews once no new coding categories emerged from the data [4].

Interviews were conducted in German, either face-to-face or online, voice or voice and video recorded. The interviewees, all of them based in Germany, covered different gender, age groups and backgrounds and had experiences with Conversational User Interfaces (CUI) (see Appendix 7.1 for detailed information on each interviewee). The interview length was planned to last around 30 minutes and varied based on the experiences of people and their willingness to share their thoughts and feelings. Based on previous research [3] and a literature review [2, 10, 11] privacy-sensitive contexts had been identified and an interview script was designed (see Appendix 7.2 for the interview script). However, the process of interviewing remained flexible and questions were rephrased or newly added as new concepts emerged throughout the interview [4].

3. Findings and Recommendations

The interview data covered different scenarios and contexts in which people disclose private information. Interviewees described HMI with regards to CUI as well as technology-enabled interactions with service providers. However, regarding the main findings these two scenarios did not differ in privacy evaluation and behavior and we will refer to them as HMI contexts.

3.1. Human-to-Human vs. Human-Machine-Interaction

While it is intuitively understood that HHI is different from HMI, we were interested in identifying distinguishing factors and potentially learning from HHI for the design of interfaces in HMI. Contextual features varied considerably across scenarios, however, reasons to disclose were consistently different. Regarding interactions between humans, I2 described *"I basically did it to open up a bit too, so that he doesn't get the impression that he has, so to speak, exposed himself and that he doesn't get anything back [...] I think the right thing to do is to be human."* Empathy and reciprocity as well as a feeling of sympathy and closeness towards the other person are the main motivators to share private information in HHI contexts. In contrast, regarding HMI, I4 stated that *"I wanted to change an appointment with my bank advisor, called a hotline and they asked for my customer number and PIN. I then had to read them out loud. [...] I was concerned to say it out loud."* Here, requirements rather than empathy and reciprocity cause people to reveal personal information. Such forcing mostly leads to negative feel-

10.21437/SPSC.2021-16

ings, such as insecurity and tension. While HHI left the interviewees with positive feelings and an association of trust towards the other person, trust was not found to play a crucial role in HMI as stated by I3 *"I don't think an institution can really be trusted. Trust towards a company, I think, it doesn't exist."* Factors like familiarity and the reason for disclosure were more important in HMI as denoted by I1 *"Yes, it depends a lot on the reason and how often I use it and whether I knew the website before."*

We claim that forcing people to reveal private information and the associated negative feelings have more impact on peoples' decisions than mistrust in HMI. Therefore, designers should thoroughly examine whether information is necessary before requiring users to share it. Currently, it is not uncommon that applications require information that is not necessary for their functioning [12]. If information is identified as necessary, designers should enable users to freely choose between different modalities to transmit compulsory information to reduce the impact of negative feelings on future usage.

Furthermore, HHI and HMI scenarios differed drastically in the way people try to and are able to self-censor themselves and use self-protective strategies. In HHI, self-censorship usually includes concealing information or avoiding to talk about sensitive topics. This flexibility is not given in HMI contexts when machines refuse to proceed if certain information is not entered. Protective strategies, in HHI, include control over physical context variables, such as securing the surrounding by closing a door or checking for familiar faces in a coffee shop. Those are usually carried out intuitively and within a short time. In HMI, this kind of control mechanisms were adopted by only few interviewees and were often not only subject to privacy but convenience considering device functionality. Generally, in HMI scenarios, protective mechanisms were more difficult, time-consuming and often required technological knowledge as stated by I4 and I1 *"Not going to certain pages on the phone. Because I am more familiar with my laptop, I am also more familiar with security mechanisms on my laptop and then I do security-related things, such as banking, rather on my laptop. What is more, I cover the cell phone camera in certain situations."* and *"If I can, I refuse and do it another way. Most of the time you can enter a city nearby or something."* The last comment supports the idea that in some cases, the need for protection leads to rejection of the service as a whole.

Based on those findings we state that there is a need for flexibility regarding user input such that users can self-censor similarly to what they are used to in HHI. Moreover, easy and quick to use protection strategies are needed in HMI.

3.2. Benefits and Costs in HMI Scenarios

As described above, people in our sample tended to act on an emotional level when connecting with humans. They did not tend to rationally assess benefits when determining whether to disclose information, which may be due to the discussed contexts, as suggested by Nissenbaum [13]. In our interviews, we found that in HMI, benefits were crucial motivators for disclosure. In the scenarios described by the interviewees, benefits were usually clear, precise and well known to them as one statement by I3 shows *"Especially with banking, there are often VoiceBots that then just verify the voice and then also look at security features, whether to authenticate the caller, to verify, and I actually think that's quite good. It brings, I think, more advantages than if someone from the call center is sitting there who has never heard me before and has no connection to me."* As expected, in many of the described HMI scenarios, the interviewees assessed both benefits and risks for decision making. However, decision making was not purely based on rational risk evaluation but rather on an interpretation based on mental models, conviction, awareness and risk assessment. Contrary to concretely nameable benefits, costs remained elusive and hard to grasp. Moreover, costs were associated with negative emotions which can lead to rejection of a service as stated by I6 *"Because I am afraid that I will be spied on. So that's [Voice Assistant] what I turned off on my cell phone and also on my PC".*

An implication for research is to identify strategies and techniques, e.g. cognitive forcing [14], to promote rational evaluation and weighing of both risks and benefits in HMI. Such strategies and techniques could help avoid immediate rejection due to irrational benefit-risk assessment and help users to make informed decisions. Moreover, techniques are desirable which support users making informed decisions by making costs and benefits more comparable, e.g. by reducing the elusiveness of costs. Methods to this goal need to be investigated in the context of CUI.

The vague interpretation of risks is closely related to uncertainty, which does not seem to be reduced by technical knowledge as it was mentioned by interviewees with and without a technical background. This is illustrated, for example, by statements made by I1 and I3: *"They always said that you should be careful what you write by email because it is stored somewhere [...] That is why you should discuss as much as possible privately and not via email. Because if you write a private email you don't know who is reading it."* and *"Or what happens if the robot now somehow loads under the table somehow and somehow records everything, like conversations or what happens in the household and so on. I often think it is this uncertainty, where eventually you ask yourself: "Do I need it then?" If I don't know what is going to happen with it and then the added value is perhaps not much greater now than if I did press five buttons on the phone or anywhere else, then I don't need that at the moment."*

4. Conclusion and Future Work

We conducted semi-structured interviews with the aim to find factors influencing feelings and behaviors linked to privacy and how they differ between HHI and HMI scenarios. We interviewed nine people. Thus our sample is small. Moreover, our demographic categories are basic. Future work should expand the number of interviewees, the documented demographic categories and design interview questions to cover privacy in context [13]. One of the reoccurring themes in our interviews was the difference of factors influencing disclosure in HHI and HMI contexts. We found that self-protective strategies are common in HHI scenarios and were intuitively carried out while people face difficulties in using proper protective mechanisms in HMI contexts which can lead to the refusal of a service as a whole. Future work could focus on the development of suitable protection strategies in different HMI contexts. While benefits and costs are known to play a crucial role in HMI scenarios, during the process, we gained deeper insight into the nature of users assessment of costs and benefits [15]. We found that users had a clear understanding of the benefits while the costs remained elusive to them. Further research is therefore needed to understand the impact of this mismatch on informed decision making and its implications for designing HMI.

5. Acknowledgments

Our work is partially funded by the German Federal Ministry for Economic Affairs and Energy as part of their AI innovation initiative (funding code 01MK20011A).

6. References

[1] Y. Javed, S. Sethi, and A. Jadoun, "Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*. Canterbury CA United Kingdom: ACM, Aug. 2019, pp. 1–10.

[2] H. Lee and A. Kobsa, "Understanding user privacy in Internet of Things environments," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. Reston, VA, USA: IEEE, Dec. 2016, pp. 407–412.

[3] B. Brüggemeier and P. Lalone, "Perceptions and reactions to conversational privacy initiated by a conversational user interface," *Computer Speech & Language*, vol. 71, p. 101269, 2022.

[4] C. Urquhart, *Grounded theory for qualitative research: a practical guide*. Los Angeles, Calif. ; London: SAGE, 2013, oCLC: ocn823891293.

[5] G. Chalhoub and I. Flechais, ""Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users," in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed. Cham: Springer International Publishing, 2020, vol. 12210, pp. 305–325, series Title: Lecture Notes in Computer Science.

[6] N. Abdi, K. M. Ramokapane, and J. M. Such, "More than smart speakers: Security and privacy perceptions of smart home personal assistants," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 451–466.

[7] F. Yeasmin, S. Das, and T. Bäckström, "Privacy analysis of voice user interfaces," in *Proceedings of Conference of Open Innovations Association FRUCT*, ser. Proceedings of Conference of Open Innovations Association FRUCT. United States: IEEE, 2020.

[8] P. K. Masur, *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Springer International Publishing AG, 06 2018.

[9] M. N. Marshall, "Sampling for qualitative research," *Family Practice*, vol. 13, no. 6, pp. 522–526, 12 1996.

[10] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner, "Privacy Attitudes of Smart Speaker Users," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 4, pp. 250–271, oct 2019.

[11] E.-M. Schomakers, C. Lidynia, D. Müllmann, and M. Ziefle, "Internet users' perceptions of information sensitivity – insights from Germany," *International Journal of Information Management*, vol. 46, pp. 142–150, Jun. 2019.

[12] M. Hatamian, V. Schmitt, and J. Nicholson, "Is your surveillance camera app watching you? a privacy analysis," *Journal IEEE Security & Privacy Special Issue on Security and Privacy Issues of Home Globalization*, Submitted.

[13] H. Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review*, vol. 79, p. 41, 2004.

[14] Z. Buçinca, M. B. Malaya, and K. Z. Gajos, "To Trust or to Think: Cognitive Forcing Functions Can Reduce Overreliance on AI in AI-assisted Decision-making," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW1, pp. 1–21, Apr. 2021.

[15] S. Barth and M. D. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics*, vol. 34, no. 7, pp. 1038–1058, Nov. 2017.

7. Appendix

7.1. Interviewees' Profile

Table 1: *Interviewees' Profile: Interviews with I7 and I8 were conducted together, Tech: technical education or working in technical fields*

I#	Gender	Age	Background	Setting	Length
I1	female	29	Non-Tech	offline	36 min
I2	female	32	Tech	online	47 min
I3	male	42	Tech	online	32 min
I4	female	N/A	Tech	online	34 min
I5	male	23	Tech	online	44 min
I6	female	27	Non-Tech	offline	25 min
I7	male	84	Non-Tech	offline	56 min
I8	female	83	Non-Tech	offline	56 min
I9	male	33	Tech	offline	25 min

7.2. Interview Script

1. Introduction: About the Interviewer, Project, Interview Rules
2. About the Interviewee
3. Definition "Private Information"
   (a) What do you think of when you hear the world "private information"?
      i. Feelings
      ii. Situations
      iii. People
   (b) Where does the definition come from?
   (c) Experience with other definitions? Cultural differences?
4. General Experience
   (a) Was there a recent situation in which you unintentionally exchanged private information with someone/a service/a machine?
      i. Description of the situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
      ii. Similar Experiences
      iii. Impact on the Future
      iv. What would have made the situation more pleasant for you?
   (b) Are there places where you would not exchange private information and why?
5. Work Context
   (a) To what extent is the work environment/office a place where you exchange private information?
   (b) What do you pay attention to in the context?
   (c) Description of a typical situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
6. Banking Context

    (a) Recent situation with a bank employee/ banking service
    (b) Description of the situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
    (c) Prior Experiences in the banking context
    (d) Impact on the Future

7. Medical Context
    (a) Attitude towards medical data
    (b) General thoughts on sharing medical information
    (c) Do you remember an uncomfortable situation related to your health data?
        i. Description of the situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
        ii. Impact on the Future
        iii. What would have made the situation more pleasant for you?
8. Company/Service Provider Context
    (a) How do you usually try to contact companies or service providers?
    (b) Is there anything you pay attention to when contacting companies or service providers?
    (c) Recent situation with a company/ service provider
        i. Description of the situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
        ii. Impact on the Future
    (d) Similar Experiences
9. Government/State Context
    (a) Have you had anything to do with government institutions?
        i. Description of the situation: Contextual features, Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
10. Can you think of anything else? To the situations that we have discussed or to other situations that occur to you in this context?
11. Conversational User Interfaces
    (a) Have you ever heard of Conversational User Interfaces? Text or Voice-Based?
    (b) Have you already had contact with Conversational User Interfaces?
        i. Context (Banking, Health, Companies/ Service Providers, Car, Smartphone, Smart Speakers)
        ii. Usage
        iii. Thoughts, Feelings, Risk, Benefits, Trust, Appropriateness
12. Is there anything else you'd like to talk about?
13. Do you have any final thoughts on the topic of Conversational User Interfaces?